

THE CYBER-DEFENCE REVOLUTION: A SYNTHESIS

Scott Borg, Director and Chief Economist, U.S. Cyber Consequences Unit

THE CYBER-DEFENSE REVOLUTION (BORG SUMMARY)		
	Industrial Defense Era	Cyber-Defense Era
Central Principles	Nation states as adversaries	Networked groups as adversaries
	Concentrated forces	Diffuse forces
	Fire power advantage	Information advantage
	Aspiring to intimidating force	Aspiring to ubiquitous force
Strategy	Defending perimeters of geographical areas from attacks originating outside	Defending internal networks and operations from attacks appearing inside
	Military and military-industrial targets	Critical infrastructure targets
	Success measured by destruction of equipment and infliction of casualties	Success measured by the protection or destruction of value
	Battlefield theory as central	Economic theory as central
	Deterrence-based policies	Resilience-based policies
Tactics	Engagements between groups of men and weapons	Engagements between integrated systems with extensive automated programs
	Concentrated blows as the central action	Complex repositioning as the central action
	Information systems as support	Information systems as weapons
	Speed and range in executing attack operations as crucial	Speed and coverage in identifying the nature and location of the adversary's operations as crucial
	Area and facility targeting	System and process targeting
	Destruction of targets	Co-option—hijacking or corruption—of targets
	Most attacks repeatable and effective even if expected	Many attacks unrepeatable and ineffective if expected
	Assured results	Probabilistic results
Decision Processes	Centralized decision-making	Flexibly distributed decision-making
	Emphasis on large group discipline	Emphasis on small group initiative
	Clarity about identity of adversary	Uncertainty about identity of adversary
	Problems with deducing patterns from insufficient information	Problems with recognizing patterns amid excess information